

## § 150.301

will assume enforcement responsibility.

### **Subpart C—CMS Enforcement With Respect to Issuers and Non-Federal Governmental Plans—Civil Money Penalties**

#### **§ 150.301 General rule regarding the imposition of civil money penalties.**

If any health insurance issuer that is subject to CMS's enforcement authority under § 150.101(b)(2), or any non-Federal governmental plan (or employer that sponsors a non-Federal governmental plan) that is subject to CMS's enforcement authority under § 150.101(b)(1), fails to comply with HIPAA requirements, it may be subject to a civil money penalty as described in this subpart.

#### **§ 150.303 Basis for initiating an investigation of a potential violation.**

(a) *Information.* Any information that indicates that any issuer may be failing to meet the HIPAA requirements or that any non-Federal governmental plan that is a group health plan as defined in section 2791(a)(1) of the PHS Act and 45 CFR § 144.103 may be failing to meet an applicable HIPAA requirement, may warrant an investigation. CMS may consider, but is not limited to, the following sources or types of information:

(1) Complaints.

(2) Reports from State insurance departments, the National Association of Insurance Commissioners, and other Federal and State agencies.

(3) Any other information that indicates potential noncompliance with HIPAA requirements.

(b) *Who may file a complaint.* Any entity or individual, or any entity or personal representative acting on that individual's behalf, may file a complaint with CMS if he or she believes that a right to which the aggrieved person is entitled under HIPAA requirements is being, or has been, denied or abridged as a result of any action or failure to act on the part of an issuer or other responsible entity as defined in § 150.305.

(c) *Where a complaint should be directed.* A complaint may be directed to any CMS regional office.

## 45 CFR Subtitle A (10–1–03 Edition)

#### **§ 150.305 Determination of entity liable for civil money penalty.**

If a failure to comply is established under this Part, the responsible entity, as determined under this section, is liable for any civil money penalty imposed.

(a) *Health insurance issuer is responsible entity—*(1) *Group health insurance policy.* To the extent a group health insurance policy issued, sold, renewed, or offered to a private plan sponsor or a non-Federal governmental plan sponsor is subject to applicable HIPAA requirements, a health insurance issuer is subject to a civil money penalty, irrespective of whether a civil money penalty is imposed under paragraphs (b) or (c) of this section, if the policy itself or the manner in which the policy is marketed or administered fails to comply with an applicable HIPAA requirement.

(2) *Individual health insurance policy.* To the extent an individual health insurance policy is subject to an applicable HIPAA requirement, a health insurance issuer is subject to a civil money penalty if the policy itself, or the manner in which the policy is marketed or administered, violates any applicable HIPAA requirement.

(b) *Non-Federal governmental plan is responsible entity.* (1) *Basic rule.* If a non-Federal governmental plan is sponsored by two or more employers and fails to comply with an applicable HIPAA requirement, the plan is subject to a civil money penalty, irrespective of whether a civil money penalty is imposed under paragraph (a) of this section. The plan is the responsible entity irrespective of whether the plan is administered by a health insurance issuer, an employer sponsoring the plan, or a third-party administrator.

(2) *Exception.* In the case of a non-Federal governmental plan that is not provided through health insurance coverage, this paragraph (b) does not apply to the extent that the non-Federal governmental employers have elected under § 146.180 to exempt the plan from applicable HIPAA requirements.

(c) *Employer is responsible entity.* (1) *Basic rule.* If a non-Federal governmental plan is sponsored by a single employer and fails to comply with an applicable HIPAA requirement, the employer is subject to a civil money

penalty, irrespective of whether a civil money penalty is imposed under paragraph (a) of this section. The employer is the responsible entity irrespective of whether the plan is administered by a health insurance issuer, the employer, or a third-party administrator.

(2) *Exception.* In the case of a non-Federal governmental plan that is not provided through health insurance coverage, this paragraph (c) does not apply to the extent the non-Federal governmental employer has elected under § 146.180 to exempt the plan from applicable HIPAA requirements.

(d) *Actions or inactions of agent.* A principal is liable for penalties assessed for the actions or inactions of its agent.

#### § 150.307 Notice to responsible entities.

If an investigation under § 150.303 indicates a potential violation, CMS provides written notice to the responsible entity or entities identified under § 150.305. The notice does the following:

(a) Describes the substance of any complaint or other information. (See Appendix A to this subpart for examples of violations.)

(b) Provides 30 days from the date of the notice for the responsible entity or entities to respond with additional information, including documentation of compliance as described in § 150.311.

(c) States that a civil money penalty may be assessed.

#### § 150.309 Request for extension.

In circumstances in which an entity cannot prepare a response to CMS within the 30 days provided in the notice, the entity may make a written request for an extension from CMS detailing the reason for the extension request and showing good cause. If CMS grants the extension, the responsible entity must respond to the notice within the time frame specified in CMS's letter granting the extension of time. Failure to respond within 30 days, or within the extended time frame, may result in CMS's imposition of a civil money penalty based upon the complaint or other information alleging or indicating a violation of HIPAA requirements.

#### § 150.311 Responses to allegations of noncompliance.

In determining whether to impose a civil money penalty, CMS reviews and considers documentation provided in any complaint or other information, as well as any additional information provided by the responsible entity to demonstrate that it has complied with HIPAA requirements. The following are examples of documentation that a potential responsible entity may submit for CMS's consideration in determining whether a civil money penalty should be assessed and the amount of any civil money penalty:

(a) Any individual policy, group policy, certificate of insurance, application, rider, amendment, endorsement, certificate of creditable coverage, advertising material, or any other documents if those documents form the basis of a complaint or allegation of noncompliance, or the basis for the responsible entity to refute the complaint or allegation.

(b) Any other evidence that refutes an alleged noncompliance.

(c) Evidence that the entity did not know, and exercising due diligence could not have known, of the violation.

(d) Documentation that the policies, certificates of insurance, or non-Federal governmental plan documents have been amended to comply with HIPAA requirements either by revision of the contracts or by the development of riders, amendments, or endorsements.

(e) Documentation of the entity's issuance of conforming policies, certificates of insurance, plan documents, or amendments to policyholders or certificate holders before the issuance of the notice of intent to assess a penalty described in § 150.307.

(f) Evidence documenting the development and implementation of internal policies and procedures by an issuer, or non-Federal governmental health plan or employer, to ensure compliance with HIPAA requirements. Those policies and procedures may include or consist of a voluntary compliance program. Any such program should do the following:

(1) Effectively articulate and demonstrate the fundamental mission of compliance and the issuer's, or non-